CLAIMS

What I claim as my invention is:

1.A method for securely submitting biometric data from a client to a server comprising the steps of:

performing sampling of a real biometric characteristic at the client; and

shuffling arrays of real biometric characteristics in the sequence known at client only to thereby generate twisted biometric data; and

submitting the twisted biometric data from the client to the server.

2. A method according to claim 1 wherein the shuffling sequence is calculated at client on the base of the value of a secret object created at the client and known to client only.

3. A method according to claim 2 combined with the step of multiplying the arrays of biometric characteristics by the sequences of numbers fixed for each type of array and known at the client only.

4. A method according to claim 3 wherein the step of submitting of twisted biometric data is followed by the step of comparing this data against the samples of twisted biometric data saved at the server previously, in such a way, that the result of the verification and/or identification depends neither on the specific sequence in which biometric arrays were shuffled on the client, nor on the specific sequence of numbers used on the client to change the values of the arrays.

5. A system for secure use of biometric data comprising:

the means for performing of twisted sampling and submitting data to the server according to claim 3; and

the means for client verification and/or identification according to claim 4.

6. A computer program product for secure use of biometric data comprising:

the computer-readable program code for performing twisted sampling and submitting data to server according to claim 3; and

the computer-readable program code for client verification and/or identification according to claim 4.